WHAT IS CLAIMED IS:

1	1. A method for providing automated tracking of security vulnerabilities,
2	comprising:
3	performing a vulnerability assessment on a system;
4	storing data obtained from the vulnerability assessment in a vulnerability
5	database;
6	determining a vulnerability score based on a plurality of vulnerability factors
7	identified by the vulnerability assessment; and
8	determining a time to fix a vulnerability identified by the vulnerability assessmen
9	of the system based on the determined vulnerability score.
1	2. The method of claim 1, wherein determining the vulnerability factor
2	further comprises considering the frequency the identified vulnerability occurs in the
3	system.
1	3. The method of claim 2, wherein determining the vulnerability factor
2	further comprises the criticality of an element in the system presenting the vulnerability
3	and a rating of the severity of the vulnerability.
1	4. The method of claim 1 further comprising determining an IP address
2	associated with the vulnerability.

1	5.	The method of claim 4 further comprising entering the IP address and a
2	description of	f the identified vulnerability in a tracking database.
1	6.	The method of claim 1 further comprising determining delinquent
2	vulnerabilitie	s based upon the determined time to fix the vulnerability identified by the
3	vulnerability	assessment.
1	7.	The method of claim 6 further comprising providing notification of
2	determined d	elinquencies.
1	8.	The method of claim 6 further comprising re-running a scan profile when
2	notification is	s received that the vulnerability has been fixed.
1	9.	The method of claim 8 further comprising determining whether the
2	vulnerability	still exists and archiving records associated with the vulnerability when the
3	vulnerability	does not still exist.
1	10.	A method for determining a criticality factor for a vulnerability in a
2	computer sys	tem, comprising:
3	enteri	ng in a database vulnerabilities identified during a vulnerability assessment;
4	moni	toring a frequency of occurrence for the identified vulnerabilities; and
5	assign	ning a vulnerability factor to a vulnerability based upon the frequency of
6	occurrence o	f the vulnerability in the system.

1	11. The method of claim 10, wherein the assigning a vulnerability factor
2	further comprises considering a criticality of an element in the system presenting the
3	vulnerability and a rating of the severity of the vulnerability within the system.
1	12. An apparatus for providing automated tracking of security vulnerabilities,
2	comprising:
3	a memory for storing program instructions; and
4	a processor, configured according to the program instructions for performing a
5	vulnerability assessment on a system, storing data obtained from the vulnerability
6	assessment in a vulnerability database, determining a vulnerability score based on a
7	plurality of vulnerability factors identified by the vulnerability assessment and
8	determining a time to fix a vulnerability identified by the vulnerability assessment of the
9	system based on the determined vulnerability score.
1 2	13. The apparatus of claim 12, wherein the processor considers a frequency of the identified vulnerability in the system when determining the vulnerability factor.
_	ino idolimino i i i i i i i i i i i i i i i i i i
1	14. The apparatus of claim 13, wherein the processor further considers the
2	criticality of an element in the system presenting the vulnerability and a rating of the
3	severity of the vulnerability when determining the vulnerability factor.
1	15. The apparatus of claim 12, wherein the processor determines an IP address

2

associated with the vulnerability.

The apparatus of claim 15, wherein the processor enters the IP address and 16. 1 a description of the identified vulnerability in a tracking database. 2 The apparatus of claim 12, wherein the processor identifies delinquent 1 17. vulnerabilities based upon the determined time to fix the vulnerability identified by the 2 vulnerability assessment. 3 The apparatus of claim 17, wherein the processor provides notification of 18. 1 the identified delinquencies. 2 The apparatus of claim 17, wherein the processor re-runs a scan profile 1 19. when notification is received that the vulnerability has been fixed. 2 The apparatus of claim 19, wherein the processor determines whether the 20. 1 vulnerability still exists and archives records associated with the vulnerability when the 2 vulnerability does not still exist. 3

l	An apparatus for determining a criticality factor for a vulnerability in a
2	computer system, comprising:
3	a memory for storing program instructions; and
4	a processor, configured according to the program instructions for entering in a
5	database vulnerabilities identified during a vulnerability assessment, monitoring a
6	frequency of occurrence for the identified vulnerabilities and assigning a vulnerability
7	factor to a vulnerability based upon the frequency of occurrence of the vulnerability in
8	the system.
1	22. The apparatus of claim 21, wherein the processor considers a criticality of
2	an element in the system presenting the vulnerability and a rating of the severity of the
3	vulnerability within the system when assigning a vulnerability factor.
1	23. An apparatus for providing automated tracking of security vulnerabilities,
2	comprising:
3	means for storing program instructions; and
4	means configured according to the program instructions provided by the means
5	for storing for performing a vulnerability assessment on a system, storing data obtained
6	from the vulnerability assessment in a vulnerability database, determining a vulnerability
7	score based on a plurality of vulnerability factors identified by the vulnerability
8	assessment and determining a time to fix a vulnerability identified by the vulnerability
9	assessment of the system based on the determined vulnerability score.

1	24. An apparatus for determining a criticality factor for a vulnerability in a
2	computer system, comprising:
3	means for storing program instructions; and
4.	means configured according to the program instructions provided by the means
5	for storing for entering in a database vulnerabilities identified during a vulnerability
6	assessment, monitoring a frequency of occurrence for the identified vulnerabilities and
7	assigning a vulnerability factor to a vulnerability based upon the frequency of occurrence
8	of the vulnerability in the system.
1	25. A program storage device readable by a computer, the program storage
2	device tangibly embodying one or more programs of instructions executable by the
3	computer to perform a method for providing automated tracking of security
4	vulnerabilities, the method comprising:
5	performing a vulnerability assessment on a system;
6	storing data obtained from the vulnerability assessment in a vulnerability
7	database;
8	determining a vulnerability score based on a plurality of vulnerability factors
9	identified by the vulnerability assessment; and
0	determining a time to fix a vulnerability identified by the vulnerability assessment
1	of the system based on the determined vulnerability score.

26. A program storage device readable by a computer, the program storage
device tangibly embodying one or more programs of instructions executable by the
computer to perform a method for determining a criticality factor for a vulnerability in a
computer system, the method comprising:
entering in a database vulnerabilities identified during a vulnerability assessment;
monitoring a frequency of occurrence for the identified vulnerabilities; and
assigning a vulnerability factor to a vulnerability based upon the frequency of
occurrence of the vulnerability in the system